UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/020,470	10/30/2001	Wei-Qiang Michael Gui	13768.209	9272

47973 7590 05/12/2009

WORKMAN NYDEGGER/MICROSOFT
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UT 84111

EXAMINER	
DEBNATH, SUMAN	

ART UNIT	PAPER NUMBER
2435	

MAIL DATE	DELIVERY MODE
05/12/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/020,470	GUI ET AL.	
	Examiner	Art Unit	
	SUMAN DEBNATH	2435	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *05 March 2009*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-9,22-25,27-35,41 and 43-50* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-9,22-25,27-35,41 and 43-50* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-9, 22-25, 27-35, 41 and 43-50 are pending in this application.

2. Claims 1, 3-9, 22-24, 27, 29-35, 41, 43 and 45 are currently amended.

3. Claims 46-50 are newly added.

4. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office Action.

Continued Examination Under 37 CFR 1.114

5. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on March 05, 2009 has been entered.

Claim Objections

6. Claims 1, 27 and 48 are objected to because of the following:

Regarding claims 1, 27 and 48, the Applicant fails to comply with the written description requirement. The claim contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventors, at the time the application was filed, had possession of the claimed invention. Specifically claims are amended to include “validating the second set of

credentials provided by the user, wherein the second set of credentials are also associated with the single unique user identifier of the user, the single unique user account, and the single unique user profile, such that the user may access the single unique user account by entering the first set or the second set of credentials".

Appropriate correction and/or clarification is required.

Claim Rejections - 35 USC § 103

7. Claims 48-50 are rejected under 35 U.S.C. 103(a) as being unpatentable over Moreh et al. (Patent No.: US 6,959,336 B2) (hereinafter "Moreh") and further in view of Bush et al. (Pub. No.: US 2002/0083012 A1) (hereinafter, "Bush").

8. As to claim 48, Moreh discloses In a system including a service that is accessed by a user from one or more devices with varying input capabilities, a method for associating multiple credentials with a single user account such that the user may be authenticated with any one of the multiple credentials (abstract), the method comprising an authentication system performing acts of:

receiving an authentication request at the authentication system from a first computer, wherein the authentication request includes a first set of credentials of the user ("[a] subject 20 may authenticate in any environment using any type of credential" e.g. see, col. 6, lines 40-56, "The authentication agent 24 can return more than one appropriate authentication mechanism 32. The client 22 therefore may have a call back mechanism to enable local determination of exactly which authentication mechanism 32

it should use", e.g. see, col. 6, lines 62-67 and col. 7, lines 1-28, “the client 22 delivers the authentication response to the server application 38", e.g. se, col. 6, lines 15-25, see also, col. 5, lines 38-55);

validating the first set of credentials provided by the user, wherein the first set of credentials are associated with a single unique user identifier of the user, and a single unique user profile (“[t]he client 22 delivers the authentication response to the server application 38", e.g. see, col. 6, lines 15-30, see also, col. 5, lines 38-55, col. 6, lines 15-30 & lines 40-67 and col. 7, lines 5-28; It should be noted that Moreh authenticates using multiple set of credentials based on the environment and device input capability, e.g. see, col. 6, lines 40-56);

receiving a second authentication request at the authentication system from a second computer, where the authentication request includes a second set of credentials of the user, the second set of credentials being different than the first set of credentials (e.g. see, col. 6, lines 15-30, see also, col. 5, lines 38-55, col. 6, lines 15-30 & lines 40-67 and col. 7, lines 5-28; It should be noted that Moreh authenticates using multiple set of credentials based on the environment and device input capability, e.g. see, col. 6, lines 40-56); and

validating the second set of credentials provided by the user, wherein the second set of credentials are also associated with the single unique user identifier of the user, and the single unique user profile (e.g. see, col. 6, lines 15-30, see also, col. 5, lines 38-55, col. 6, lines 15-30 & lines 40-67 and col. 7, lines 5-28; It should be noted that Moreh

authenticates using multiple set of credentials based on the environment and device input capability, e.g. see, col. 6, lines 40-56).

Although Moreh teaches an authentication system wherein the user uses a callback mechanism to select one authentication mechanism from a plurality of choices (col. 7, lines 5-15), Moreh may not explicit abut having a single unique user account such that user may access the single unique user account by entering either the first set or the second set of credentials.

However, Bush discloses a single unique user account such that user may access the single unique user account by entering either the first set or the second set of credentials ("within one account, different sets of credentials (e.g. different user name and password) can be used to access different or even the same resource", e.g. see, [0022]).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Moreh as taught by Bush in order to minimize the complexity of user account maintains by multiple devices in different environments.

9. As to claim 49, the combinations of Moreh and Bush disclose wherein the first and second computer are the same computer, and wherein the first set and second set of credentials comprise a username and password, and wherein the username of the first set of credentials is different than the username of the second set of credentials (Bush: [0022]).

10. As to claim 50, the combinations of Moreh and Bush discloses wherein the username of first set of credentials is an email address having a first domain and the username of the second set of credentials is an email address having a second domain that is different than the first domain (Moreh: col. 7, lines 29-55).

11. Claims 1, 9, 27, 35 and 45-47 are rejected under 35 U.S.C. 103(a) as being unpatentable over Moreh and further in view of Bush and Quinlan et al. (Patent No.: US 6,748,365 B1) (hereinafter, "Quinlan").

12. As to claim 1, Moreh discloses in a system including a service that is accessed by a user from one or more devices with varying input capabilities, a method for associating multiple credentials with a single user account such that the user may be authenticated with any one of the multiple credentials (abstract), the method comprising an authentication system performing acts of:

receiving an authentication request at the authentication system from a desktop computer, wherein the authentication request includes a first set of credentials of the user, the first set of credentials comprising a username and a password (e.g. see, col. 6, lines 15-30, see also, col. 5, lines 38-55, col. 6, lines 15-30 & lines 40-67 and col. 7, lines 5-28; It should be noted that Moreh authenticates using multiple set of credentials based on the environment and device input capability wherein credentials includes user ID/passwords on a computer or a hand-held device, e.g. see, col. 6, lines 40-56),

validating the first set of credentials provided by the user, wherein the first set of credentials are associated with a single unique user identifier of the user and a single unique user profile ("[t]he client 22 delivers the authentication response to the server application 38", e.g. see, col. 6, lines 15-30, see also, col. 5, lines 38-55, col. 6, lines 15-30 & lines 40-67 and col. 7, lines 5-28; col. 6, lines 40-56);

receiving a second authentication request at the authentication system from a cellular phone, wherein the authentication request includes a second set of credentials of the user, the second set of credentials (e.g. see, col. 6, lines 15-30, see also, col. 5, lines 38-55, col. 6, lines 15-30 & lines 40-67 and col. 7, lines 5-28; It should be noted that Moreh authenticates using multiple set of credentials based on the environment and device input capability, wherein credentials includes user ID/passwords on hand-held device, e.g. see, col. 6, lines 40-56); and

validating the second set of credentials provided by the user, wherein the second set of credentials are also associated with the single unique user identifier of the user, and the single unique user profile, (e.g. see, col. 6, lines 15-30, see also, col. 5, lines 38-55, col. 6, lines 15-30 & lines 40-67 and col. 7, lines 5-28).

Although Moreh teaches an authentication system wherein the user uses a callback mechanism to select one authentication mechanism from a plurality of choices (col. 7, lines 5-15), Moreh may not explicit about set of credentials comprising a numeric username and a numeric pin, wherein the numeric username is distinct from the username and having a single unique user account such that user may access the

single unique user account by entering either the first set or the second set of credentials.

However, Bush discloses a single unique user account such that user may access the single unique user account by entering either the first set or the second set of credentials ("within one account, different sets of credentials (e.g. different user name and password) can be used to access different or even the same resource", e.g. see, [0022]).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Moreh as taught by Bush in order to minimize the complexity of user account maintains by multiple devices in different environments.

Although Bush discloses different sets of credentials (e.g. different user name and password) which can be used to access the same resource ([0022]), neither Moreh nor Bush may not explicitly disclose set of credentials comprising a numeric username and a numeric pin.

However, Quinlan discloses set of credentials comprising a numeric username and a numeric pin ("[t]he customer may have an alphanumeric username and password for use via computer and a numeric username and password for user by telephone", e.g. see, col. 14, lines 9-12).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Moreh and Bush as taught by Quinlan for simplicity (Quinlan, col. 14, lines 8-9).

13. As to claim 27, it is rejected using the similar rationale as for the rejection of claim 1.

14. As to claim 46, the combinations of Moreh, Bush and Quinlan disclose wherein the user selects which set of credentials to provide from among a plurality of sets of credentials valid at the authentication system and associated with the user, the set of credentials being chosen by the user based at least partially on the user's device, the method further comprising: receiving a new set of credentials from the user, wherein the new set of credentials is associated with the same unique user identifier of the user, user account and user profile; storing the new set of credentials in a credential store of the authentication system such that the authentication system can authenticate the user to the service when the user provides any one of multiple sets of credentials associated with the user account; and providing, in response to the request, the unique user identifier and the user profile to the device (Moreh teaches an authentication system wherein the user uses a callback mechanism to select one authentication mechanism from a plurality of choices; Moreh: e.g. see, col. 6, lines 15-30, see also, col. 5, lines 38-55, col. 6, lines 15-30 & lines 40-67 and col. 7, lines 5-28).

15. As to claim 47, it is rejected using the similar rationale as for the rejection of claim 46.

16. As to claim 9, the combinations of Moreh, Bush and Quinlan disclose wherein the unique user account corresponds to a service, the method further comprising: receiving an authentication response from the authentication system, wherein the authentication response includes the unique user identifier that authenticates the user to the service, the response also including the user profile; and sending an authenticated request to the service, wherein the authenticated request includes the unique user identifier and user profile such that access to the service is obtained (Moreh: e.g. see, col. 6, lines 15-30, see also, col. 5, lines 38-55, col. 6, lines 15-30 & lines 40-67 and col. 7, lines 5-28).

17. As to claim 35, it is rejected using the similar rationale as for the rejection of claim 9.

18. As to claim 45 the combinations of Moreh, Bush and Quinlan disclose wherein the act off validating the first and second sets of credentials provided by the user further comprises an act of the authentication system comprising the first and second sets of credentials selected by the user against the plurality of sets of credentials stored in the credential store to determine validity (Moreh teaches an authentication system wherein the user uses a callback mechanism to select one authentication mechanism from a plurality of choices; Moreh: e.g. see, col. 6, lines 15-30, see also, col. 5, lines 38-55, col. 6, lines 15-30 & lines 40-67 and col. 7, lines 5-28).

19. Claims 2-3, 8, 22, 28-29 and 34 are rejected under 35 U.S.C. 103(a) as being unpatentable over Moreh and further in view of Bush, Quinlan and Wood et al. (Patent No.: US 6,609,198 B1) (hereinafter "Wood").

20. As to claim 2, nether Moreh nor Bush and Quinlan explicitly disclose wherein the authentication system is a distributed authentication system, wherein the act of receiving an authentication request at the authentication system further comprises an act of determining where to send the credentials for validation. However, Wood discloses wherein the authentication system is a distributed authentication system, wherein the act of receiving an authentication request at the authentication system further comprises an act of determining where to send the credentials for validation (col. 17, lines 15-25).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Moreh, Bush and Quinlan as taught by Wood in order to provide enhanced security to the credential repository with location transparency.

21. As to claim 28, it is rejected using the similar rationale as for the rejection of claim 2.

22. As to claim 3, the combinations of Moreh, Bush, Quinlan and Wood disclose wherein the act of determining where to send the credentials for validation uses a username of the credentials (Wood: col. 17, lines 15-25).

23. As to claim 29, it is rejected using the similar rationale as for the rejection of claim 3.

24. As to claim 8, the combinations of Moreh, Bush, Quinlan and Wood disclose a step for remembering which set of credentials was received in the authentication request (Wood: col. 10, lines 25-65); a step for prompting the user for a more secure set of credential when the set of credentials received in the authentication request do not meet security requirements of the service (Wood: col. 10, lines 25-65); and a step for providing at least one security measure for each set of credentials associated with the user account, wherein the user is not authenticated to a service if the security measure of a particular set of credentials is breached or the user account is locked (Wood: col. 10, lines 30-35).

Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Moreh, Bush and Quinlan as taught by Wood in order to provide credentials without loss of session continuity.

25. As to claim 34, it is rejected using the similar rationale as for the rejection of claim 8.

26. As to claim 22, the combinations of Moreh, Bush, Quinlan and Wood disclose wherein the new set of credentials has an associated security level and wherein the user has attempted to authenticate using the first set of credentials and wherein the method further comprises:

associating the new set of credential with the user account such that the user can be authenticated with any of the plurality of sets of credentials (Wood: col. 10, lines 25-65),

prior to providing the response, and subsequent to receiving the authorization request, prompting the user for a secure set of credentials that is more secure than the original credential if the security level of the first set of credentials is insufficient for a service being accessed by the user, wherein the service is provided with the security level of both the first set of credentials and the secure set of credentials, but is not aware of either the first set of credentials or the secure set of credentials (Wood: col. 10, lines 25-65).

27. Claims 4-5, 30-31, 41, 43-44 are rejected under 35 U.S.C. 103(a) as being unpatentable over Moreh and further in views of Bush, Quinlan and Sweet at al. (Pub. No.: US 2002/0031230 A1) (hereinafter “Sweet”).

28. As to claim 4, nether Moreh nor Bush and Quinlan explicitly disclose wherein the act of receiving new credentials from the user further comprises an act of symmetrically

associating the new credentials with a unique user identifier. However, Sweet discloses wherein the act of receiving new credentials from the user further comprises an act of symmetrically associating the new credentials with a unique user identifier ([0025], [0026], [0039], lines 4-7, [0040], lines 20-26).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Moreh, Bush and Quinlan as taught by Sweet in order to "provide a system design which is substantially more compatible with a broad number of Internet-based applications in the corporate information protection, content vending, entertainment, and telecommunications (wireless systems) fields (Sweet, [0020])."

29. As to claim 30, it is rejected using the similar rationale as for the rejection of claim 4.

30. As to claim 5, the combinations of Moreh, Bush, Quinlan and Sweet disclose wherein the act of symmetrically associating the new credential with a unique_user identifier further comprises an act of associating the new credentials with a user account (Sweet: [0025], [0026], [0039], lines 4-7, [0040], lines 20-26).

31. As to claim 31, it is rejected using the similar rationale as for the rejection of claim 5.

32. As to claim 41, the combinations of Moreh, Bush, Quinlan and Sweet disclose wherein the same unique user identifier is provided to the user regardless of the set of credentials received from the user (Sweet: [0026], [0028], [0039], lines 4-7, [0040], lines 20-26).

33. As to claim 43, the combinations of Moreh, Bush, Quinlan and Sweet disclose wherein providing the unique user identifier and the user profile to the device comprises sending a cookie containing the unique user identifier and the user profile to the device (Sweet: [0026], [0039], lines 4-7, [0040], lines 20-26).

34. As to claim 44, the combinations of Moreh, Bush, Quinlan and Sweet disclose wherein the user profile includes data about the user comprising name, personal information, preferred language, preferences, and location (Sweet: [0026], [0039], lines 4-7, [0040], lines 20-26).

35. Claims 7 and 33 are rejected under 35 U.S.C. 103(a) as being unpatentable over Moreh and further in views of Bush, Quinlan and Leah et al. (Patent No.: US 6,986,039 B1) (hereinafter “Leah”).

36. As to claim 7, neither Moreh nor Bush and Quinlan explicitly disclose wherein the act of receiving new credentials from the user further comprises an act of asymmetrically associating the new credentials with a primary credential, wherein the

primary credential is stored in a primary store with the unique user identifier. However, Leah discloses wherein the act of receiving new credentials from the user further comprises an act of asymmetrically associating the new credentials with a primary credential, wherein the primary credential is stored in a primary store with the unique user identifier (FIG. 3, col. 10, lines 48-67 to col. 11, lines 1-10).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Moreh, Bush and Quinlan as taught by Leah in order to synchronize credentials securely and propagate among multiple directories, operating system platforms and registries.

37. As to claim 33, it is rejected using the similar rationale as for the rejection of claim 7.

38. Claims 6 and 32 are rejected under 35 U.S.C. 103(a) as being unpatentable over Moreh and further in views of Bush, Quinlan, Sweet and Laursen et al. (Patent No.: 6,065,120) (hereinafter “Laursen”).

39. As to claim 6, neither Moreh nor Bush, Quinlan and Sweet explicitly disclose wherein the act of symmetrically associating the new credential with a unique user identifier further comprises an act of caching a copy of the unique user identifier with the new credential. However, Laursen discloses wherein the act of symmetrically associating the new credential with a unique user identifier further comprises an act of

caching a copy of the unique user identifier with the new credential (FIG. 2b, col. 8, lines 4-35).

Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Moreh, Bush, Quinlan and Sweet as taught Laursen in order to perform transactions or retrieve pertinent information without the need to key in such every time the transactions or the information are desired.

40. As to claim 32, it is rejected using the similar rationale as for the rejection of claim 6.

41. Claims 23-25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Moreh and further in views of Bush, Quinlan, Wood and Leah.

42. As to claim 23, the combinations of Moreh, Bush, Quinlan, Wood and Leah disclose wherein the step for associating new set of credentials with the user account further comprises a step for symmetrically associating the fist set of credentials and the new set of credentials with the user account, wherein the user account is cached with each of the first set of credentials and the new set of credentials (Leah: col. 10, lines 48-67 to col. 11, lines 1-10). Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Moreh, Bush,

Quinlan and Wood as taught by Leah in order to synchronize credentials securely and propagate among multiple directories, operating system platforms and registries.

43. As to claim 24, the combinations of Moreh, Bush, Quinlan, Wood and Leah disclose wherein the step for associating the new set of credentials with the user account further comprises a step for asymmetrically associating the new set of credentials with a primary set of credentials, wherein the primary set of credentials is associated with the user account and wherein the primary set of credentials is cached with each new set of credentials (Leah: col. 10, lines 48-67 to col. 11, lines 1-10).

44. As to claim 25, the combinations of Moreh, Bush, Quinlan, Wood and Leah disclose wherein the step for associating the new set of credentials with the user account further comprises a step for asymmetrically associating the new set of credentials with a primary set of credentials, wherein the primary set of credentials is associated with the user account and wherein the primary set of credentials is cached with each new set of credentials (Leah: FIG. 3, col. 10, lines 48-67 to col. 11, lines 1-10).

45. **Examiner's note:** Examiner has cited particular columns and line numbers in the references as applied to the claims above for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures

may be applied as well. It is respectfully requested from the applicant, in preparing the responses, to fully consider the references in entirety as potentially teaching all or part of the claimed invention as well as the context of the passage as taught by the prior art or disclosed by the examiner.

Response to Arguments

46. Applicant's arguments with respect to claim 1-9, 22-25, 27-35, 41 and 43-50 have been considered but are moot in view of the new ground(s) of rejection.

Conclusion

47. Any inquiry concerning this communication or earlier communications from the examiner should be directed to SUMAN DEBNATH whose telephone number is (571)270-1256. The examiner can normally be reached on 8 am to 5 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y. Vu can be reached on 571 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/S. D./
Examiner, Art Unit 2435

/Kimyen Vu/

Supervisory Patent Examiner, Art Unit 2435